14th District • New York

Congresswoman

Carolyn Maloney

Reports

2430 Rayburn Building • Washington, DC 20515 • 202-225-7944
1651 Third Avenue • Suite 311 • New York, NY 10128 • 212-860-0606

Statement of Congresswoman Carolyn B. Maloney
Field Hearing on the Certification and Testing of Electronic Voting Systems
May 7, 2007

I would like to thank Chairman Clay for holding this hearing today, and for traveling all the way to be here this morning. I appreciate all the hard work done by the gentleman and his staff on an issue that is very important to me -- the accuracy and security of the nation's voting systems.

In recent years, considerable concern has been expressed about the security and reliability of electronic voting systems. Reports from governmental agencies, testimony before Congress, and academic studies have indicated serious vulnerabilities that call for immediate attention.

Penetration testing done by independent computer security experts has demonstrated that election results can be altered in a manner that cannot be detected by normal election security procedures. Independent reviews commissioned by state election officials have revealed serious security vulnerabilities in the software architecture of voting systems now in use.

Typically, when concerns about the security and reliability of voting systems are raised, supporters argue that these systems have been tested to Federal standards. However, at a recent hearing of this subcommittee, the Government Accountability Office (GAO) reported that "the tests performed by independent testing authorities and state and local election officials do not adequately assess electronic voting systems' security and reliability. These concerns are intensified," they continued, "by a lack of transparency in the testing process." The GAO noted weak and insufficient system testing, source code reviews, and penetration testing. They pointed out that most of the systems that exhibited the weak security controls had been nationally certified after testing by an independent testing authority.

Last summer the EAC undertook a review of the laboratories that had been testing under the NASED program. The Assessment Report of one of those labs, CIBER, concluded, "CIBER has not shown the resources to provide a reliable product." The report also noted "CIBER's reports provide limited or no descriptions of the testing performed so a reader or reviewer can not tell if all the testing was completed." Here in New York an independent review of CIBER's test plans revealed that they did not document the methodologies, procedures and processes necessary to ensure that all testing is done in a structured and repeatable way.

It is estimated that CIBER has tested the software in more than 70% of the voting machines used last November. "Estimated" because there's no way to know for sure which lab tested which system. And apparently there is also no way of knowing for sure if any testing was done at all.

Trusting the word of the ITA, election officials across the country used taxpayer money to purchase equipment believing that this equipment was in conformance with Federal standards. Apparently we have no way of knowing whether the equipment actually does meet Federal standards. CIBER hides behind a cloak of confidentiality. Because test methods are considered proprietary, the public and election officials cannot verify that procedures are done properly.

When a system fails a test, there's no public announcement. Further, if the system subsequently passes, there's no way to identify what changes the manufacturer made, if any, to enable the system to pass. Considering that CIBER certified 70% of the machines in use last November, we have a real dilemma. Do we keep using machines that were certified by an ITA that did not meet the standards for accreditation or do we have to start over and recertify? I'm glad that CIBER will be here today to respond to our concerns.

The national testing and certification program has been vital to the sales and acceptance of voting systems in most states. Experience is often the best test – and a lot of jurisdictions are finding problems with the machines that the ITAs seem to have missed. Several states that moved forward quickly to buy touch screen voting machines are realizing that the machines they bought don't work very well. New Mexico decided to switch to optical scan-style voting statewide in 2006, including in four counties that spent a total of $4 million for touch-screen machines. Last month Maryland switched to optical scan. This month Florida followed suit.

New York is looking pretty smart these days – by focusing on standards and refusing to jump quickly into untested technology, our election officials may have saved taxpayers a lot of money.

We need meaningful testing to make sure equipment meets the 2005 standards. This hearing provides an opportunity to examine the current state of voting system testing and certification in this great nation. It can also serve as a step towards a more transparent and trustworthy process in the future.

Unless we improve our certification process, we are in dangering of losing the confidence of American voters.